# 第 56 回 IETF ミーティング参加報告書

富士ゼロックス株式会社
稲田 龍
セコムトラストネット
島岡政基
NPO 日本ネットワークセキュリティ協会
安田直義
富士ゼロックス情報システム株式会社
増田健作

2003/3/17-21 に米国サンフランシスコの San Francisco HILTON にて開催された第 56 回 IETF(Internet Engineering Task Force: http://www.ietf.org/ )ミーティング に NPO 日本ネットワークセキュリティ協会(略称: JNSA http://www.jnsa.org/)が 2002 年度に情報処理振興事業協会セキュリティセンター(略称: IPA/ISEC http://www.ipa.go.jp/security/) より委託を受けた事業である JNSA Challenge PKI 2002 プロジェクトの報告とその成果物である"Multi Domain PKI Test Suite"のデモンストレーションを PKIX-WG にて行う目的で JNSA 安田直義氏、セコムトラストネット島岡政基氏および FXIS 増田健作氏と共に参加したので報告する。

第 56 回 IETF ミーティングの参加者は 34 カ国から 325 の組織で、総勢 1,640 人であった。アトランタの第 55 回 IETF ミーティングの参加者は 34 カ国から 334 の組織で、総勢 1,706 人であった。横浜の第 54 回 IETF が 2,064 人、第 53 回のミネアポリスの IETF が 1,756 人であった。同時テロ以前のロンドンで行われた第 51 回 IETF が 2,457 人であったことを考えるとテロの影響と米国における IT バブルの崩壊の影響と思われる。

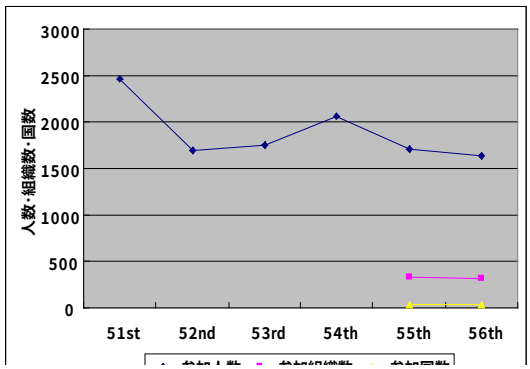


図 1 IETF ミーティング参加人数の推移

# 概観

## 報告者の PKIX-WG での発表に関して

報告者である稲田は、アトランタで行われた第 55 回 IETF に引き続き JNSA と共同で行っている「JNSA Challenge PKI 2002」の報告とその成果物である”Multi Domain PKI Test Suite”のデモンストレーションを PKIX-WG で報告した。

PKIX-WG の報告に関しては、P.18の「PKIX」を参照のこと。

写真 1 PKI-WG ミーティングで報告している稲田(右)

「JNSA Challenge PKI 2002」プロジェクトおよび”Multi Domain PKI Test Suite”は、IPA/ISEC の平成 14 年度「情報セキュリティ関連の調査・開発に関する公募」に対して JNSA が応募し採択された「電子政府情報セキュリティ相互運用支援技術の開発」によるものである。

発表内容は、「JNSA Challenge PKI 2002」の概要(P.3の図 2)と成果物である”Multi Domain PKI Test Suite”のコンセプトと機能概略(P.3の図 3)の説明および今後、Multi Domain PKI 環境を定義し、テスト環境を作るための Internet-Drafts を書く事を報告した(報告を行った資料は付録として添付)。

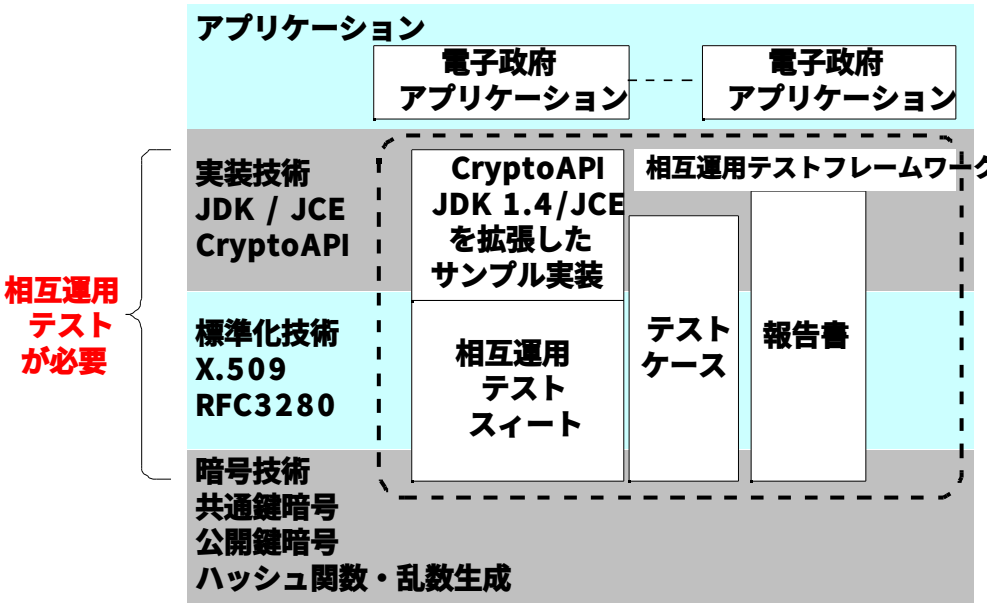


図 2 JNSA Challenge PKI 2002 の概要

日本政府は、行政手続きの効率化と国民負担の軽減を目標に、国民と行政機関の間の申請・届出・通知などといった手続きを電子化する「電子政府」の構築を目指している。

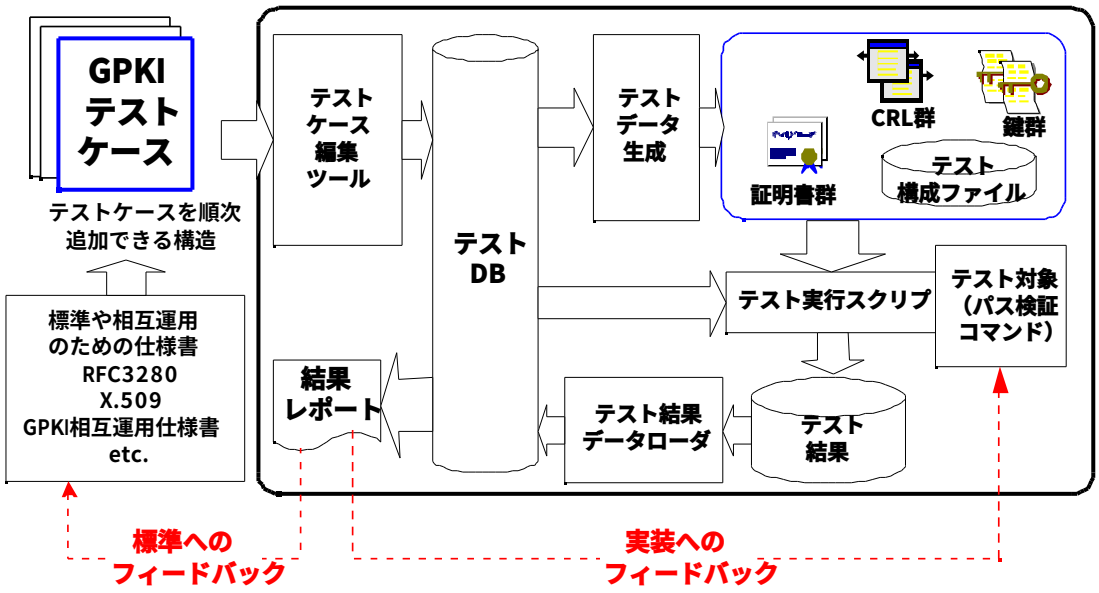


図 3 “Multi Domain PKI Test Suite”の概要

情報流通の基盤として構築されている政府認証基盤(GPKI) では、ブリッジ CA モデルと呼ばれる信頼モデルが使用されている。ブリッジ CA モデルは、主体者が異なるマルチドメイン PKI

を実現する手段として柔軟性のあるモデルであるが、その反面、ドメイン間での相互運用性を確保するために高度な技術を要する。

その状況下で、適正な PKI アプリケーションの開発を行うために証明書の失効確認/パス検証を行うテスト環境として ”Multi Domain PKI Test Suite”とテストケースを開発した。 ”Multi Domain PKI Test Suite”は GPKI に限らず、汎用な PKI テスト環境を提供する。

現在、インターネット上では PKI のアプリケーションが使われているが、複雑な PKI ドメインを適用している例は少ない。また、PKIX が出した RFC 3280 では、複雑な PKI ドメインを使うことも考慮されてはいるが実際に試せる環境は少ない。NIST などで RFC 3280 の相互接続実験は行われているが、テスト環境の構築が難しく手軽にテストすることは難しい。

今回の”Multi Domain PKI Test Suite”は、スタンドアロンで動作し手軽にテスト環境を構築/運用できるようにしたものであり、他に類がない。「JNSA Challenge PKI 2002」の報告書を英訳および”Multi Domain PKI Test Suite”の公開を 6 月に公開する事を発表した。

また、この”Multi Domain PKI Test Suite”を作るにあたって Multi Domain PKI の定義が IETF では文書化されていない事が明らかになった。Multi Domain PKI 環境でのテストケースを適正に作成維持していくためには「Multi Domain PKI の定義」を文書化し共通の認識で作成していく必要性を実感したため、「Multi Domain PKI の定義」の Internet-Drafts 化を行うことと、テストケースを交換しやすくするためにテストケースデータベースのスキーマの定義をする Internet-Drafts を作成するつもりであると報告した。

写真 2 質問をする Steve Hanna 氏

発表後の Q&A では、Sun Microsystems 社 Steve Hanna 氏(JAVA JDK の PKI 検証ライブラリの作成者 )が、発表に使用したスライドがいつ公開されるかという質問があった (スライドは PKIX-WG のチェアには送付済みで、後日、Proceedings として公開される予定)。

写真 3 Tim Polk 氏と

ミーティング終了後、台湾の Panasonic Taiwan Laboratories の周立平氏/陳柏飛氏がコンタクトして来た。彼らも Multi Domain PKI 環境でのテストを行うことに苦慮しており、公開の時期と彼らの環境で動くかどうかを気にしていた。

ミーティングの終了後、Tim Polk 氏と今後の活動に関しての議論を行った。作成を意図している 2 つの Internet-Drafts は、WG ドキュメントにするか JNSA のパーソナルドキュメントではじめるかに関わらず 7 月の PKIX-WG での議論対象にすることも可能であることを確認した。

また、発表後に Glenn Mansfield Keeni 氏(P.15/Extended Incident Handling(INCH)の主要メンバー)より以下の共同で行える事がないかという趣旨のメールをもらった。

> Subject: Todays PKIX Presentation
> From: Glenn Mansfield Keeni glenn@cysols.com
> To: Ryu Inada <Ryu.Inada@fujixerox.co.jp>
> Dear Inada-san,
> That was good and important work ! What are the plans from now. Let me know if I can help in any way.
> We are looking forward to the presentation in Vienna.
> Cheers
> Glenn

# IETF における PKI の応用

前回のアトランタで行われた第 55 回 IETF ミーティングでも、話題として上げられていたが、PKI を S/MIME や SSL/TLS 以外のアプリケーション/プロトコルでも利用する動きがある。

実際、AAA-WG で決まった Diameter においてはデータの交換形式として CMS(Cryptographic Message Syntax)を用いて暗号化/電子署名が実現されている。

今回の S/MIME-WG のミーティングにおいても SIP のパケットフォーマットに CMS を使うという動きがある(P.14の「S/MIME Mail Security」を参照)。

PKI の利用範囲が広まりつつある反面、なかなか配備が進まない、技術的に難解であると言う不満が出ている(P.19の「Open Security Area Directorateを参照」。これらの状況は、ようやく PKI が「インターネットで使える技術」として認知されたということである。

また、今回の「IESG Open Plenary」(P.17)で正式に発表されたが、Security Area の Director として長年貢献した MIT の Jeffrey I. Schiller 氏に代わり、元 RSA Laboratories(現 Virgil Security 社)の Russell Housley 氏が就任した。Housley 氏は RFC 2459/3280 の著者の一人であり PKI の第一人者である。この交代は、3 年近く PKIX-WG の活動を通じ、PKI の展開を進めていたが、この展開が遅々として進まない反面、OASIS/W3C/EESI などから続々と PKI に対しての標準の提案と IETF に対しての協調の要請が出ている状況を IESG としては看破できず、PKI に対してのてこ入れがなされたと報告者は受け取った。前節にも述べたとおり、PKI が「インターネットで使える技術」として認知こともあり、今後の展開が期待される。

# IETF の在り様の変化

IETF は、インターネットの標準の策定を行っているが、昨今、活動範囲が多岐にわたり他組織との間の協調の必要性が高くなっており、 IETF が独自に規約/標準を決められなくなりつつある。これは、インターネットが複雑化し多くの団体がその価値を認め利用を始めていることの証明である。

また、IETF の内部にも問題を抱えている。

第一に、IETF の運営資金をどうするかが問題となりつつある。IETF は、いくつかの資金源を持っているが、多くは年 3 回の IETF オフラインミーティングの会費で賄っている。ここ数回のオフラインミーティングの参加者が落ち込んでいる状況を考えると楽観は出来ない。実際、過去からの繰越金で運営されている状態であり 3 年後には資金が枯渇するとの報告があった。また従来、IETF のオフラインミーティングには、スポンサーが付くが(第 54 回の横浜の IETF では、富士通がスポンサーとなった)、今回のオフラインミーティングでは初めての試みとしてスポンサーなしでオフラインミーティングが行われた。これは、米国での IT 業界の不況のためスポンサーのなり手がなかったのではないかとも、また、特定のスポンサーの利害に IETF が左右されるのを嫌ったとも考えられる。

第二に、IETF が標準化を行う領域が広く、また細分されており IETF に参加しているメンバーのレビューが出来なくなりつつある。具体的には、各 WG から提出される Internet-Drafts のレビュー率が低くなり(平均 10%程度)、Internet-Drafts として IESG が承認できない状況が増えている事が報告されている。これは Internet-Drafts の内容が高度に専門化されてしまい、多くのメンバーは何が書いてあるかが理解できていない状況であるといえる。

詳細は、P.17の「IESG Open Plenary」および P.20の「Open IAB Plenary」を参照のこと。

# IETF におけるセキュリティに対する意識

IETF においても、セキュリティは大きな問題として取り上げられており、「セキュリティ」はひとつのキーワードとなっている。

具体的には、RFC/Internet-Draft には Security Consideration というセクションが設けられており RFC の発行に関して Area Director/IESG(Internet Engineering Steering Group)から「セキュリティに関しての考察が甘い」といったコメントがある場合が多い。

IETF の初日である 17 日には、Security Tutorial が開かれ、Security Area の Area Director である Jeffrey Schiller 氏/Steven Bellovin 氏より Protocol を安全に設計するためのチュートリアルが開かれた(詳細は P.11の「写真 7 講演する Jeffrey I. Schiller 氏

Security Tutorial」を参照のこと)。この Security Tutorial は昨今の IETF では毎回開催されている。

また、IETF の会期の終わり近くに「Open Security Area Directorate」があり、IETF およびインターネットにおけるセキュリティのあり方の議論と現状の報告が行われる (詳細は P.19の「Open Security Area Directorate」を参照のこと)。

今回の「Open Security Area Directorate」では、PKI が話題となっていた。PKI は、3 年にわたって展開を行おうとしているが、うまく展開できていないのはなぜであるかが話題となっている。

IETF ミーティングではターミナルルームと無線 LAN でのネットワークコネクティビティを提供しており、すべてのコンファレンスルームでインターネットへ自由に接続できる。前回の IETF ミーティングでは、IETF 主催者側より「無線 LAN においてパケットの盗聴の可能性があるので SSL/SSH/IPsec など暗号化を行うこと」という注意が流れている。今回の IETF では、IETF の Web 上(http://www.ietf.org/meetings/netinfo.html)に以下の注意が載せてある。

**Security Warning**

Please note that using 802.11 without additional encryption is not private. In particular, do not use protocols with cleartext passwords, such as telnet or non-APOP POP3. Instead, use encrypted protocols such as SSH, SSL or IPsec. It is well-known that people may be sniffing packets on the network. There should be no expectation of privacy when using unencrypted protocols on the IETF-56 network.

EAP で無線 LAN の認証とセキュリティに関しての議論がなされている一方で、この様にある意味では無防備なネットワーク環境が用意されているところに IETF のひとつの側面が現れている。インターネットは、自由なネットワークアクセス環境を提供する。その上で自己を守るための枠組みを作り、それを利用するか否かは利用者が決めるべきであるという考えである。

# IETF のネットワーク環境とターミナルルーム


写真 4 ターミナルルーム 左側: 入り口/右側: 全景

IETF では、インターネットの利用を行うためターミナルルームが用意されているが、ここ数回の IETF において通例となっている無線 LAN(IEEE 802.11b)によるネットワークアクセスが提供されており、会場およびその周辺では自由にネットワークアクセスを行うことが出来た。そのためか、今回のターミナルルームはいつものターミナルルームに比べ狭く感じた (写真 4 右)。

会場となったホテルのロビーおよびバーにおいてもこの無線 LAN を使うことが出来たためロビーのそこかしこでノート PC を持った参加メンバーがインターネットに接続していた。また、ロビー/バーで食事を取りながら打ち合わせをする姿も多く見られた。

写真 5 ホテルのロビーにて

ターミナルルームは SUN Microsystems が運営をしており、SUN RAY を持ち込んでいた。SUN RAY を使うために、SMART CARD が配られており、この CARD には固有の UID が書き込まれており、ユーザ毎の SUN RAY の設定情報を呼び出すのに使われているとの事であった。

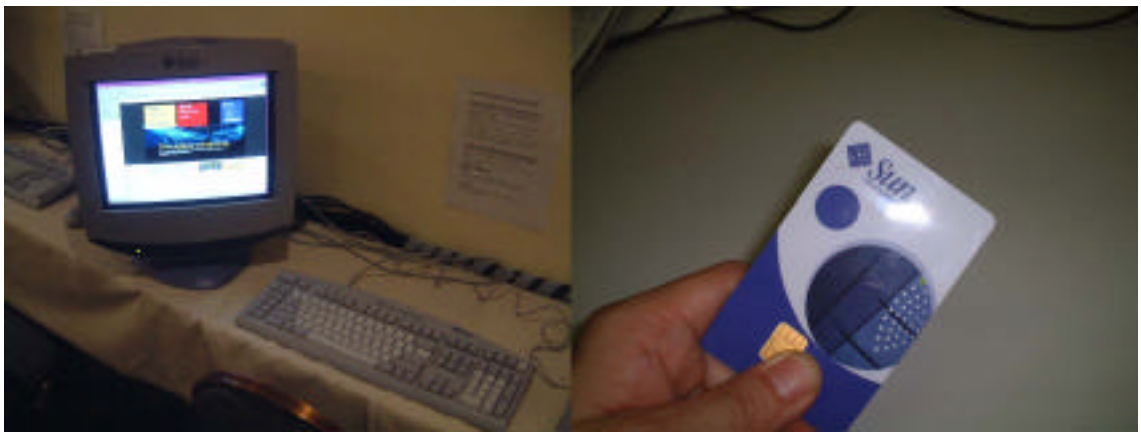

写真 6 SUNRAY(左)と SMART CARD(右)

# WG 概観

## New comer orientation & IETF Standard Process Orientation

本セッションは、IETF の組織や標準の作られる過程について Steve Coya 氏から説明が行われた。

IETF の組織には、まずテーマ毎に召集される Working Group(WG)が存在する。各 WG はその技術適用範囲によりエリア分け(現在は 8 つのエリアが存在する)され、各エリアにはエリアディレクターと呼ばれる専門の技術者が配置されている。そして各エリアを統括するための上位組織として IESG(Internet Engineering Steering Group)が存在する。IESG は IETF のチェアおよび各エリアのエリアディレクターで構成される。

WG は、大風呂敷を広げたものより目的を絞ったもの、余計なオプションのないものを重視し、"Rough consensus and running code"(大雑把な合意と動くコード)を作ることを基本としている。WG はアウトプットとして RFC(Requests For Comments)とよばれる技術文書を作成する。RFC にはいわゆる標準過程 (Standard Track)文書の他に、 Best Current Practices, Informational, Experimental, Historic と呼ばれるものがある。

標準を作るためには、まず Internet Draft が作成される。ここで標準化する事となった場合は、標準過程に入りまず Proposed Standard が作成され 6 ヶ月(〜2 年)意見が求められ、さらに Draft Standard が作成され 4 ヶ月(〜2 年)意見が求められ、Standard となる。各プロセスにおいて、Proposed Standard ではデモ実装、Proposed Standard では複数の独立した相互通信可能な実装、さらに Standard においては安定して動作するいわゆる本物("The real thing")が求められる。ここでも実装のない机上の空論のようなものは認めないという、IETF の目的重視の姿勢が見られる。このような標準化プロセス自身も RFC 化(RFC2026)されている。

WG 自体は、まず検討すべきテーマがあった時に技術者が集まり BOF(Bird Of Feather)と呼ばれるグループが作成される。そこでのテーマや活動方針がそのエリアのエリアディレクターに認められ、さらに IAB および IESG に承認されることにより WG となる。現在では約 80%の BOF が WG となっている。

セッションに参加した人の多くは初めて IETF ミーティングに参加する人たちであった。IETF ではすべてオープンに検討しておくことが重視され、何をやるにしても何か提案したら "step away from the table"が重要と繰り返し説明されていた。

# Security Tutorial

本セッションはセキュリティのエリアディレクターである Jeffrey I. Schiller(MIT)と Steve M.

写真 7 講演する Jeffrey I. Schiller 氏

ュリティの基礎的な紹介である。

ンターネットが抱えるセキュリティ脅威としてアタ

,DoS,etc)の一般的な話があり、この脅威に対抗する

由は技術面でもそうだが、エンドユーザー側の意識

は"negative deliverable"であり、Schiller 氏の母親は

ないと言うと会場が笑いに包まれた)

術的な対抗手段として、暗号化、暗号方式(DES,AES)、

の適用範囲(通信路を守る IPsec,通信データ自身を守

る S/MIME)、認証モデルなどが紹介された。

Schiller 氏によるとセキュリティの "Perfect World"は、「すべてのユーザ/ホストが証明書を持ち、通信路は IPsec/TLS で守られ、アプリケーションは最適なセキュリティ技術を使用し、パスワードがそのまま流れないようにする」ということだった。

これに対し現状は、IPsec の適用範囲は通信路に限られかつまだ準備段階であり、証明書は普及に困難しているとした。また、名前空間にしても X.509,DNS,E-Mail 間でばらばらで、何らかの規約が必要であること、認可 (authorization)に関してもクライアント/サーバーでは単純だが、複数パーティーでの権限委譲などにおいて問題があることが指摘された。

写真 8 新 Director Russell Housley 氏

最後に今回新しくエリアディレクターとして紹介された Russell Housley(Vigil Security)が、セキュリティの設計面での要件として大事なことは、単純さ (simplicity)であると訴えた。複雑なセキュリティは、設計、実装、利用の各段階において困難さがつきまとうためである。「バグを作りがちなセキュリティシステムは、よりハッカーに侵入される!」という指摘は、あたり前ではあるが設計者としては身につまされた。

セキュリティは IETF において昨今の一番の関心ごとである一方、問題としても取り上げられている。後日行われた「IESG Open Plenary」においても、プロトコル設計初期段階からセキュリティ要件を満たすべく設計を行うことをエンジニアに求めていた(ただし実情は厳しいようだ。P.19の「Open Security Area Directorate」参照)。IETF 初日において Security Tutorial が独立したセッションとして最初に行われるのは、このような背景と問題意識の表れである。

# Applications Open Area

本セッションはアプリケーションエリア全体での問題を話し合う目的で召集されたものである。

今回は議論の大半が、IPv6 からのサイトローカルのアドレス解決の問題点が説明された。

IPv6 のユニキャストには、リンクローカル、サイトローカル、グリーバルの 3 レベルがあるが、サイトローカルについては定義が不明確ということであった。サイトローカルではアドレス情報がサイト境界にて失われてしまうことに伴い、end-to-end での通信で支障をきたす場合がある。IPv6 の WG 内でこのサイトローカル問題を解決する議論されており、サイトローカルのアドレス解決を制限することが紹介された。ただし、この方法によるとサイトローカルアドレスを識別するための ZoneID というものが必要になり、アプリケーションにはこの ZoneID を管理するための UI が新たに必要になること、サイトローカルアドレスが漏れないような対策が必要なことが指摘された。

参加者であるアプリケーションエリアのエンジニアには、解決手法の有効性、弊害、別の解決方法について意見が求められたが、彼ら自身問題をよく理解できていない様子であった。ただし、UI の変更は既存アプリケーションへの影響、エンドユーザーの混乱、本来トランスポートレベルで解決すべき問題であると、否定的な意見が支配的であった。

# Secure Neighbor Discovery(SEND)

SEND-WG は、IPv6 においてルータを検索するための基本となるプロトコルである Neighbor Discovery において、偽ルータをデフォルトルータとして選択してしまうと、この偽ルータによりパケットの盗聴、利用不能に陥る可能性があり、それをどう排除するかを主眼にした WG である。特に、IPv6 では IPsec が含まれているため IPsec でセキュリティ上安全にするためには何らかの安全な Neighbor Discovery が必要となる。

draft-ietf-send-psreq.txt に関して、last call 時にいくつかのマイナーな問題の他に 2 つの大きな問題があった事が報告された。

一つ目は”trust”という言葉の使い方で、この言葉が各所に別のコンテキストで使われているため混乱を招くということであった。結局、コンテキストに合わせて"delegation"、 "authorized" などの適切な言葉に変更することになった。コンテキストにあわせた適切な言葉の候補を Bill Sommerfeld 氏が 3/28 までにあげることとなった。

二つ目は、SEND が採用した解決策以外の解決策をドラフト上に残すか否かであり、これはドラフト上に解決策例として残すこととなった。

Cryptographically generated IPv6 addresses(CGA)において自己署名証明書をどう使うかという議論があった。このアイデア自身は、Ericsson/Microsoft の知的財産となっているが Chair が Microsoft と交渉中であると報告された。

技術的な観点から言えば、IPv6 のアドレスにハッシュ値を入れる場合、62bit までしか入れられず安全なハッシュ値とは言えない事が指摘されている。draft-aura-cga-00.txt ではこの制限をなくすため security parameter と second hash を提案している。この提案により、アドレス生成のコストはかかるが、攻撃のコストも同様に上がり安全性が保てるという事が報告された。ちなみに、アドレスの検証のコストは一定でありこの提案を入れたことによる実害はない。

draft-ietf-send-ipsec-00.txt に関しては、現在、デザインチームが考えていることのスナップショットが説明された。

このドラフトは巨大なものとなる事が予想されており、いくつかのパートに分けるべきとの意見が出た。Chair の判断により CGA の部分は分けることになった。

transition scheme に関していくつかの未解決部分がある事が確認された。

技術的な問題は、ここ数ヶ月中にデザインチームが解決することになると報告された。

# IP Version 6(IPv6)

7,8 割の聴衆。

IPv6 のプリフィックス配布について特に問題なく RFC 化されそうであると報告があった。

DHCPv6 については last call が行われ特に大きな問題もなく IESG に送られる予定。

IP/UDP/TCP MIB についてはドラフトを読んでいる人がいず議論にならない。必要性のみが確認された。

IPv6 のアドレス解決方法は IAB で不明確であることが理由に差し戻しとなった。

"Prefix router advertisement"のアクセス制御については議論が紛糾した。これは SEND との絡みもあり、今後も紛糾しそうな感がある。

IPv6 ノードの要求事項では DHCP のサポートについて議論された。ステートレスな自動コンフィグレーションがすべてのケースにおいて有効でない限り、ステートフルな自動コンフィギュレーションをサポートすべきという提案がされた。DHCP のサポートについては、実装者から意見が多く出され紛糾した。

MobileIP に関しては、特に紛糾もなく報告が行われた。

セキュリティについては、DES のサポートは MUST ではあるが、DES の安全レベルは指摘されているとおりで、下位互換のためサポートとすることが推奨されていた。

これに対し、活発な意見交換がされ紛糾した。内容は不明確。

AH と ESP の利用方法の明確について、特になし。

# S/MIME Mail Security(S/MIME)

2,3 割の聴衆。

Russell Housley(Vigil Security)がセキュリティエリアのエリアディレクターとなったため、WG のチェアが Blake Rambsdell と Sean Turner に変更となった。

S/MIME WG は、22 の RFC を発行しており、 CMS Symmetric Key Management and Distribution(symkeydist)が現在、RFC Editor の処理待ちである。Securing X.400 Content with S/MIME(x400wrap)、Transporting S/MIME Objects in X.400(x400transport)、Wrapping an HMAC key with a Triple-DES Key or an AES Key(hmac-key-wrap)、Use of the RSAES-OAEP Key Transport Algorithm in CMS(cms-rsaes-oaep)、Use of the AES Encryption Algorithm in CMS(aes-alg)が IESG のコメント待ちである旨が報告された。

まずインターネットドラフトの S/MIMEv3.1 の Certificate Handling(CERT)と Message Specification(MSG)の状況報告があった。その後、CMS のインターオペラビリティテストの途中経過が報告された。どちらも特に問題はないようであった。

そして RSA-PSS 署名対応についての報告がされた。こちらには細かな問題あるようである。

そもそも RSA 暗号のバックアップなら DSA で十分なのになぜ PSS 対応を行うべきか？という質問が出たが、PKCS#1 で正式にサポートされたもので対応する必要があるという回答が行われていた。

トランスポートエリアから SIP(Session Initiation Protocol)での S/MIME 利用についての説明があった。これは SIP のパケットの内容を暗号化/電子署名を行いという要望があり、フォーマットとして S/MIME で用いている CMS(Cryptographic Message Syntax)を利用したいということである。

従来、CMS は電子メールの暗号化/電子署名の利用を主眼に考えられてきたが電子メール以外で PKI を用いた暗号化/電子署名に利用する事例が増えているという事を示している。すでに AAA-WG で定めた Diameter においても CMS の利用がオプションではあるが認められている。

日本の Kido Akira(NTT Software)から S/MIME における Camellia(128bit 共通鍵暗号)対応と、NESSIE(New European Schemes for Signatures, Integrity, and Encryption)プロジェクトの紹介があった。

最後に MLA のトピックがあった。

# IP Security Protocol(IPSec)

7 割ぐらいの入り

まず、ESPv2,AH v2,RFC2401 についての状況報告があった。数ヶ月前に WG ラストコールがあったが、マルチキャストにおいて問題があった

IKEv2 のコンフィギュレーションペイロードについて説明があったが詳細不明。

(1) DHCP over Ipsec

(2) mode CFG over IKE

(3) DHCP over IKE

の選択肢の中で(3)の方法提案することが説明された。

IKEv2 の問題点が話された。そろそろこの問題に決着をつけることが司会から促された。議論が白熱したのは提供形式で"Suite"なのか"A la carte"なのかだったが、結論は出ない。

id payload , cert payload で紛糾。

DHCP vs. configuration payload でも紛糾。

ただし、IKEv2 は 4/15 にラストコールを行い、次回 IETF ミーティングまでには RFC を発行することを目標とすることがアナウンスされた。

# Authentication, Authorization and Accounting(AAA)

Diameter が RFC として制定された事が報告された。

鍵配布の問題について説明がされた。

セキュリティについては考察が進まないが、セキュリティエリアディレクターが協力することで進めていくことになった。

# Extended Incident Handling(INCH)

40 人ほどの出席者。

Incident Handling の重要性を説いた draft-ietf-inch-requirements-00.txt に対して WG 内での合意が取られ、要求事項に関しての要求も合意に達した。この Internet-Drafts は、draft-glenn-inch-req-00.txt と draft-ietf-inch-iodef-rfc3067bis-requirements-0.txt を統合した位置づけのものになる。

Data Model に関してのドラフトは前回のアトランタでのミーティングとウプスラで行われた Intermediate ミーティングとの指摘事項を修正したバージョンのドラフトを 3 月中に submit の予定。

今後の(攻撃的な)予定が発表された。

APR 03 Initial I-D of the implementation guidelines document

SEP 03 Submit requirements I-D to the IESG as Informational

SEP 03 Submit incident data language specification I-D to the IESG as Proposed Standard

NOV 03 Submit implementation guidelines I-D to the IESG as Informational

Glenn Mansfield Keeni/Yuri Demchenko 両氏より FINE(Format for INcident data Exchange)に対する要求事項の提案の発表があった(発表に用いられたスライドは、http://www.ietf.org/proceedings/03mar/slides/inch-1/index.html に公開されている)。

両氏の発表は、FINE のフレームワークとオペレーションモデルに対する要求事項の提案であり、SNMP の MIB をベースに考えられているように感じた。

FINE の実装である IODEF に関して同様にデータフォーマットの説明と XML のセキュリティ機構を使って IODEF のデータの機密性/完全性を行うべきであるという趣旨の発表があった。この中でも XML の電子署名の話題が取り上げられており(XML の電子署名は PKI の電子署名を使う)、この影響で IODEF のデータフォーマットの一部を変更すべきという意見であった。XML の電子署名は RFC3275 に記述がある。

# Simple Authentication and Security Layer(SASL)

SASL の Base Spec.を作成中であるが、著者が意欲をなくしてしまい新たな著者をアサインした。Base Spec.のセキュリティに対しての考察が IESG のレビューに耐えられるかが疑問視されている。

Anonymous(draft-ietf-sasl-anon-00.txt)は、WG の last call 中に修正点があがり Base Spec.と共に WG ML に投稿される予定。Sam Hartman が last call での修正点の概要を著者とレビュー後 WG ML に投稿する予定。

SASL のユーザ名/パスワードとして利用できる文字列に関してスペックを定義した SASLprep(draft-ietf-sasl-saslprep-00.txt)に問題点が提起されている。

SASLprep はユーザ名として user@domain-name を扱わねばならないがドメイン名などで使われている nameprep と微妙に定義が異なりユーザ/実装者に混乱を招く点が指摘されている。

SASLprep と Kerberos で名前空間を共有できない点が指摘された。Authorization name と Authentication name の扱いの議論が行われた。 Larry Greenfield はアプリケーションは Authorization name/Authentication name が同じであるはずと主張したが、Kurt は LDAP においては Authorization identifiers/Authentication identifiers が違う例がある事を指摘した。そのため、SASLprep に Authorization name と Authentication name をどう扱うかに関しての考察が必要という結論となった模様である。

SASL で扱う DIGEST 認証(draft-ietf-sasl-rfc2831bis.txt)で MD5 を使うことに関しての議論があった。現在、以下の 2 つの問題点がある事が報告された。

(1) AES 暗号への対応

AES 対応をマンダトリィにするか否かの判断は、セキュリティ分析後に行うことになった。セキュリティ分析の結果は WG の ML に投稿される。

(2) SASLprep に DIGEST-MD5 を入れる必要がある

SASL で扱う CRAM(Challenge-Response Authentication Mechanism)に MD5 を使う件に関しては、DIGEST-MD5 同様に SASLprep に CRAM-MD5 を入れる必要がある事が報告された。

GSSAPI の定義に関しては Base Spec.ドラフトの last call 後に GSSAPI のドラフトを last call する旨が報告された。

Individual submissions(SRP)に関しては、Sam Hartman が OID を含んだ構造体定義をすることにより GSSAPI ベースで利用可能できるという発言を行っていた。

# Protocol for carrying Authentication for Network Access(PANA)

PANA の仕様が変更されたことにより議論が活発に行われた。

今までの使用では、認証の初期段階において認証/認可手続きのみが可能な IP アドレスを配布し、その上で認証/認可手続きを行った後に利用制限がない IP アドレスを配布することとしていた。これは 802.1X が認証した後に IP アドレスを配布するために無線アクセスポイントなどではアクセスポイント自身が 802.1X に対応する必要があるという問題回避のためとしていた。

このことに対して議論が紛糾したが、すでに ML で議論されてきたことの繰り返しとなるということで、話が紛糾していた。

また、コネクション切断などにより認証を再度行う場合についての説明がされたが、紛糾した。

# IESG Open Plenary

IETF チェアの Harald Alvestrand から、今回の参加者の報告、NOMCOM、表彰が行われた後、IETF の財政状況についての報告がされた。

現状は赤字で、貯金で維持を行っているが、3 年後には貯金も底を尽きてしまうのでどうしたらよいか？という意見募集があった。聴衆からさまざまな意見が出て、スポンサーを探すべき、ライセンス料を取るべき、経費節減すべきなどさまざまな意見が出された(T シャツビジネスなどの冗談もあった。これは今回の IETF ミーティングがスポンサーレスミーティングであるため恒例の T シャツが配られなかったことに対しての皮肉も含まれている)。IETF ミーティングの参加費用の値上げ(現在の$450 から$700 へ)についてアンケートが取られたが、大多数は値上げしても参加することを表明していた。

またプライバシー問題について説明があり、プロトコル設計者にプライバシー問題を考慮してほしい旨が説明された。プライバシー侵害は、セキュリティ技術面での問題がなくとも起こ

りうる(例えば、プロトコル上問題がなくとも、実装上ローカルに保存されたプライバシーデータなどから漏れる可能性がある)ことが説明された。また、ユーザ自身が保存するデータの保護についてはユーザ任せで保護が不足しがちになることが指摘された。プロトコル設計者には、プライバシー問題が発生しないよう、設計段階の初期からプライバシー保護を念頭におくことが望まれた。

最後に、IETF 自身の問題が討議された。組織は大きくなっているが、WG メンバーの質が低下していることを指摘する声が多く寄せられた。(例えば、WG ミーティング参加者の中で提案文書を呼んでいる人がほとんどいないなど) また、この問題に関連し、発行される RFC 自体の品質も悪くなっており品質管理をどのように行うのか？また成功事例の共有などがうまく行えていないなどが問題としてあげられた。

## PKIX

今回 PKIX WG は、直前 4 日前までアジェンダが配信されず開催が一時危ぶまれるなどの懸念はあったものの、5 日目(3/20)の午前中に無事開催され、76 人の参加があった。

写真 9 PKIX のチェア Stephen Kent 氏(左)と Tim Polk 氏(右)

PKIX-WG の Co-Chair である Tim Polk 氏よりドキュメントステータスとして、現在 19 本の Internet-Draft を抱えており、DPD/DPV プロトコル(RFC 3379)に選出された SCVP(Simple Certificate Validation Protocol <draft-ietf-pkix-scvp-11.txt>) と お よ び PC(Internet X.509 Public Key Infrastructure Proxy Certificate Profile <draft-ietf-pkix-proxy-04.txt>)の 2 つが近々Last Call がかかっており RFC 化されそうであると報告された。

また、pkixrep(Internet X.509 Public Key Infrastructure Repository Locator Service <draft-ietf-pkix-pkixrep-01.txt>)が Area Director へ差し戻されることになった。

今回のメイントピックは、上述した DPD/DPV プロトコルの選出に関する報告と、選出された SCVP に関する現在の執筆状況の報告であった(WG セッション 2 時間半のうち、30 分以上をこれらに割いていた)。

DPD/DPV プロトコルの選出は、今年の 1 月下旬に、CVP(Certificate Validation Protocol)、DPD/DPV over OCSP、SCVP などの認証パス検証プロトコルに関する Internet-Draft に対して、PKIX メーリングリスト上で投票が行われた。この結果、SCVP は投票数の過半数を獲得したことに加え、RFC3379 に最も近い仕様であり、また実装経験も十分豊富であるとの理由から選定された。

既出の Internet-Draft である PC では、新たに Proxy Certificate を考慮したパス検証アルゴリズムについて追記されており、現在 Last Call 待ちの状態である。

SIM(Internet X.509 Public Key Infrastructure Subject Identification Method <draft-ietf-pkix-sim-00.txt>)に関して現在の執筆状況の報告があった。

SIM は前回 Atlanta で発表された Internet-Draft で、今までのレビュー内容を 3 月末までに改訂する、とのことであった(4 月 3 日現時点ではまだ上梓されていない)。

また、今回初見の Internet-Draft である pkalgs(Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <draft-ietf-pkix-rsa-pkalgs-00.txt>)に関しては、 PKCS#1 の version1.5 で規定されている RSASSA-PSS や RSAES-OAEP などのアルゴリズムに関して、PKI の中での利用方法を示したものであり、活発な議論が交わされていた。

TAP(Trusted Archive Protocol <draft-ietf-pkix-tap-00.txt>)についても発表が行われた。

TAP は TAA(Trusted Archive Authority)のトランザクションを定義し、アーカイブ情報の表記方法を示すものである。

TAP については、セッション中で一度は WG ドラフトとして扱わないことになったものの、その後 PKIX のメーリングリスト上で WG ドラフトとすべきかどうかについて議論が再燃し、現在も継続中である。

これら WG で扱っている Internet-Draft に関する報告の他、リエゾンパートナーからの発表として同じく IETF の ldapbisWG から PKI に関連した問題点の報告や、 EESSI(European Electronic Signature Standardization Initiative)から欧州電子署名標準化に関する活動報告が行われ、また JNSA からは、Challenge PKI 2002 の活動報告およびデモンストレーションなどを報告者の一人である稲田が行った(詳細は P.2の「報告者の PKIX-WG での発表に関して」を参照)。

今回の PKIX では、JNSA も含めてリエゾンの参加が多かったことが大きな特徴である。これは PKI がインターネットにおけるインフラとして、IETF に限らず世界中の各団体や関連する技術とお互いに強調しながら展開していく上での大きな流れであるように感じた。

# Open Security Area Directorate

セキュリティエリア全体の会合として、新しくエリアディレクターとなった Russell Housley(元 RSA Data Security 社、現Vigil Security)の紹介および各 WG から状況報告があった。

その後、インターネットエリアからの EAP(Extensible Authentication Protocol)のコンパウンド認証の問題が説明された。問題は EAP がクライアント<-->認証サーバーの間でトンネリングするとき"Man-in-the-middle"アタックが発生し、認証サーバーからのトンネル鍵が盗まれる可能性があるということである。この問題を解決するための手段として、トンネルの出入り口を暗号バインドすることで盗聴を検知し、盗聴があった場合には認証サーバーからトンネル鍵を渡さなくするという方法が提案された。出席者からトンネル自体をなくし、直接やりとりを行えば？という質問があったが、市場で使われている RADIUS 認証が簡単にはなくならないだろうことからこのようなハイブリッドな認証を行う必要があることが説明された。

公開討論においてはセキュリティエリアの問題点がいくつか指摘された。

暗号や認証/認可に関しては設計がなされるが、その後のアクセス制御についてはアプリケーション任せになりがちで結果として問題が残るのでは？という指摘。また、プロトコル設計においてセキュリティを考慮することが指示されているが、他のエリアの WG では技術的・時間的に彼らのみでは行えず、セキュリティエリアのエンジニアの援助を求めている。これに対しては、以前よりセキュリティアドバイザーを置く、個人レベルのボランティアが行われてきてはいるが、本業の WG の課題もあるなか限界があることが訴えられた。何らかのオペレーションが望まれるが、絶対的なセキュリティエンジニア不足が根底にあるため早急な解決策はなさそうであった。

また、PKI は技術的な優劣はともかくとして、PKI は敷居が高く、利用しにくいので何とかしてほしい(例えば個人で WEB サーバーにサイト証明書を使うのにベリサインに年間$300 も払うのでは利用できないなど)という要望が出された。micro-PKI, lightweight-PKI なるものがあればいい、実装上の問題として処理できるのでは？など意見が出されたが、 PKIX にディレクターの Tim Polk(NIST)からも明確な回答はなく、今後の課題問題として残された。

# Open IAB Plenary

IIJ 技術研究所の萩野純一郎氏が IAB メンバーとして就任した。日本人としては慶應義塾大学の村井純教授に続いて二人目である。

萩野氏は、 IPv6 の設計/開発で中心メンバーとして活動をしておりその功績が認められたと考えられる。実際、今回の IETF ミーティング終了後も荻野氏は直接帰国をせず、Apple 社により Max OS X での IPv6 の対応に関しての打ち合わせを行った模様である。

萩野氏の IAB 就任は、IETF が今後も IPv6 の開発とインターネットへの配備を行う事を明確に示したともいえる。

以上